REMARKS

In the non-final Office Action, the Examiner rejected claims 1-5 and 7-27 under 35 U.S.C. § 102(b) as anticipated by Phelps (U.S. Patent No. 5,602,906); rejected claims 28-35 and 51-66 under 35 U.S.C. § 103(a) as unpatentable over Phelps; and rejected claims 6 and 36-50 under 35 U.S.C. § 103(a) as unpatentable over Phelps in view of Bowman (U.S. Patent No. 5,627,886).[1]

By this Amendment, Applicants amend claims 1, 6, 7, 9-15, 17, 18, 23, 27, 28, 30, 36, 54, 55, and 66 to improve form, and cancel claims 4 and 34, without prejudice or disclaimer of the subject matter thereof. No new matter is believed to have been added by way of the present Amendment. Claims 1-3, 5-33, and 35-66 are pending.

REJECTION UNDER SECTION 102(b) BASED ON PHELPS

On page 2 of the Office Action, the Examiner rejected claims 1-5 and 7-27 under 35 U.S.C. § 102(b) as allegedly anticipated by Phelps. Applicants respectfully traverse the rejection with regard to the claims presented herein.

First, the present application has an effective filing date of April 21, 1995, based upon its dependency on U.S. Patent Application Serial No. 08/426,256 (now U.S. Patent No. 5,854,834). Accordingly, Phelps is not a proper Section 102(b) prior art reference since Phelps did not issue until February 11, 1997. Applicants address the rejection of claims 1-5 and 7-27 based on Phelps assuming that the Examiner meant to apply the reference under 35 U.S.C. § 102(e).

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references) is not concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such in the future.

A proper rejection under 35 U.S.C. § 102 requires that a single reference teach every aspect of the claimed invention either expressly or impliedly. Any feature not directly taught must be inherently present. In other words, the identical invention must be shown in as complete detail as contained in the claim. See M.P.E.P. § 2131. Phelps does not disclose or suggest the combination of features recited in claims 1-5 and 7-27, as presented herein.

Amended independent claim 1, for example, is directed to a method for detecting fraud in one of a credit card or debit card system. The system generates network event records, where each network event record is generated in response to an event in the system. The method includes the steps of: performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system; generating a fraud alarm upon detection of suspected fraud by the at least one fraud detection test; correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud; and responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case.

Phelps does not disclose or suggest the combination of features recited in claim 1. For example, Phelps does not disclose or suggest a method for detecting fraud in one of a credit card or debit card system, or performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system, as required by claim 1. Instead, Phelps discloses a fraud detection system for use in a telecommunications system to detect unauthorized use of billing numbers (col. 1, lines 6-10). Indeed, the words "debit card" do not appear in Phelps, and the words "credit card" only appear in Phelps in connection with a billing number of the telecommunications system (col. 2, line 49). Nowhere does Phelps

disclose or remotely suggest a method for detecting fraud in one of a credit card or debit card system, or performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system, as required by claim 1.

The Examiner alleged that Phelps discloses performing at least one fraud detection test on the network event records, and cited col. 1, lines 1-15 and 30-39 of Phelps for support (Office Action, page 2). Applicants respectfully disagree with the Examiner's interpretation of Phelps.

Col. 1, lines 1-15 of Phelps discloses:

TOLL FRAUD DETECTION SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

> The present invention relates to the field of telecommunications. More particularly, the invention is concerned with a detection system that analyzes call placement information concerning toll calls for detecting unauthorized use of billing numbers. In the preferred embodiment, a set of artificial intelligence rules operate on the call placement information to develop an indication that the use of a particular billing number is unauthorized.

2. Description of the Prior Art

This section of Phelps discloses a detection system for a telecommunications system that analyzes calls and detects unauthorized use of billing numbers. Nowhere in this section, or elsewhere, does Phelps disclose or suggest a method for detecting fraud in one of a credit card or debit card system, or performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system, as required by claim 1.

At col. 1, lines 30-39, Phelps discloses:

SUMMARY OF THE INVENTION

> The toll fraud detection system of the present invention solves the prior art problems discussed above and provides a distinct advance in the state of the art. More particularly,

> the invention hereof provides a rapid and highly accurate means for detecting unauthorized use of billing numbers, and for preventing further unauthorized use.

In this section, Phelps discloses that the toll (i.e., telecommunications) fraud detection system provides a means for detecting unauthorized use of billing numbers and for preventing unauthorized use. Nowhere in this section, or elsewhere, does Phelps disclose or suggest a method for detecting fraud in one of a credit card or debit card system, or performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system, as required by claim 1. Indeed, Phelps cannot disclose this feature of claim 1 because the reference is limited to telecommunications systems.

Since Phelps is limited to a telecommunications fraud detection system, Phelps cannot disclose the other features recited in claim 1, such as generating a fraud alarm upon detection of suspected fraud by the at least one fraud detection test; correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud; and responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case.

The Examiner alleged that Phelps discloses generating a fraud alarm upon detection of suspected fraud by the at least one fraud detection test, and cited Fig. 2 and col. 2, lines 40-67 of Phelps for support (Office Action, page 2). Applicants respectfully disagree with the Examiner's interpretation of Phelps.

Col. 2, lines 40-67 of Phelps discusses Fig. 2 and discloses:

> FIG. 2 in combination with FIG. 1 illustrates the method of operation of apparatus 10. Switch computers 14 receive CDRs from the coupling to links 60. As those skilled in the art appreciate, the CDR includes all of the necessary billing information including origination and termination telephone numbers, start and stop times, call duration, and type of billing. The type of billing includes whether the call was placed by direct

> distance dialing or by use of a billing number such as credit card and type (e.g. Visa), collect call, third party number, an interexchange carrier (IXC) calling card such as a FONcard, or a local exchange carrier (LEC) calling card. The CDR information received by switch computers 14 from link 60 includes data concerning direct distance dialed calls. These are not of interest in the preferred embodiment of apparatus 10 which is concerned with detecting unauthorized usage of billing numbers. Thus, each switch computer 14 is configured to delete the CDR information concerning direct distance dialed calls. Each switch computer 14 also analyzes the CDRs based on a set of expert system rules for the detection of fraudulent call activity, and generates alerts based on the CDRs to send to central computer 20 for further analysis.
>
> SCPMS 44 processes call attempt information and produces alerts that are provided to SCPMS gateway 18. These alerts are generated for LEC and IXC calling cards only when the number of attempts to use a calling card exceeds a predetermined threshold.

This section of Phelps discloses that the detection system detects fraudulent call activity (i.e., telecommunications) and generates alerts. Nowhere in this section, or elsewhere, does Phelps disclose or suggest generating a fraud alarm upon detection of suspected fraud by the at least one fraud detection test in a method for detecting fraud in one of a credit card or debit card system, as further required by claim 1.

The Examiner alleged that Phelps discloses correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, and cited col. 2, lines 30-40; col. 2, line 63 – col. 3, line 5; and col. 4, lines 40-50 of Phelps for support (Office Action, page 2). Applicants respectfully disagree with the Examiner's interpretation of Phelps.

Col. 2, lines 30-40 of Phelps discloses:

> Apparatus 10 receives call placement information and customer information from network 12. This information is used to update the history information stored in apparatus 10. Apparatus 10 generates an indication of unauthorized use of a billing number by applying the call placement and history information to a set of expert system rules. The indication is a case that is generated from an alert and assigned a priority. The case is resolved by a set of expert system rules or a researcher, and network 12 acts on the resolution.

This section of Phelps discloses that the detection system applies the call placement and

history information to set of expert system rules to determine an indication of unauthorized use. Nowhere in this section, or elsewhere, does Phelps disclose or suggest correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

Col. 2, line 63 – col. 3, line 5 of Phelps discloses:

> SCPMS 44 processes call attempt information and produces alerts that are provided to SCPMS gateway 18. These alerts are generated for LEC and IXC calling cards only when the number of attempts to use a calling card exceeds a predetermined threshold. The threshold is dependant in part on the type of product and the geographic dispersion of the call origination points. SCPMS gateway 18 analyzes the alerts based on a set of expert system rules for the detection of fraudulent call activity, and generates alerts based on the SCPMS alerts to send to central computer 20 for further analysis.

This section of Phelps discloses that the detection system generates alerts when attempts to use a calling card exceed a predetermined threshold. Nowhere in this section, or elsewhere, does Phelps disclose or suggest correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

Col. 4, lines 40-50 of Phelps discloses:

> The expert system rules are configured empirically on the basis of actual cases of unauthorized billing number usages. With this approach, the rules can be continuously updated and refined to reflect learning experiences concerning newly detected cases of toll fraud, and customized for each type of billing number. Thus, those skilled in the art will appreciate that the rules are not fixed, but are continuously evolving in order to adapt to the most current conditions.

This section of Phelps discloses that the detection system uses expert system rules that may be updated to reflect learning experiences concerning newly detected toll fraud. Nowhere

in this section, or elsewhere, does Phelps disclose or suggest correlating fraud alarms based on common aspects of the fraud alarms, the correlated fraud alarms being consolidated into a fraud case, the fraud case being assigned a priority based on a severity of the suspected fraud, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

The Examiner alleged that Phelps discloses responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case, and cited col. 2, lines 30-40; and col. 2, line 63 – col. 3, line 5 of Phelps for support (Office Action, page 3). Applicants respectfully disagree with the Examiner's interpretation of Phelps.

Col. 2, lines 30-40 of Phelps is reproduced above. This section of Phelps discloses that the detection system applies the call placement and history information to set of expert system rules to determine an indication of unauthorized use. Nowhere in this section, or elsewhere, does Phelps disclose or suggest responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

Col. 2, line 63 – col. 3, line 5 of Phelps is reproduced above. This section of Phelps discloses that the detection system generates alerts when attempts to use a calling card exceed a predetermined threshold. Nowhere in this section, or elsewhere, does Phelps disclose or suggest responding to the fraud case with a fraud prevention action, the fraud prevention action being based on the priority assigned to the fraud case, in a method for detecting fraud in one of a credit card or debit card system, as required by claim 1.

For at least these reasons, Applicants submit that claim 1 is not anticipated by Phelps. Claims 2, 3, 5, and 7-27 depend from claim 1 and are, therefore, not anticipated by Phelps for at

least the reasons given with regard to claim 1.[2] Claims 2, 3, 5, and 7-27 are also not anticipated by Phelps for reasons of their own.

For example, claim 19 recites that the at least one fraud detection test includes a comparison of at least a portion of the network event records to a predetermined pattern to identify a normal usage and/or a fraudulent usage, where the predetermined pattern is generated by a neural network. Phelps does not disclose or suggest the combination of features recited in claim 19.

The Examiner alleged that Phelps discloses the features of claim 19, and cited col. 1, lines 15-20 of Phelps for support (Office Action, page 6). Col. 1, lines 15-22 of Phelps discloses:

> In the field of telecommunications toll fraud, it is important to have advanced toll fraud prevention techniques. Prevention is especially important when the unauthorized use is for international calls because the interexchange carrier handling the call may have to transfer payments to the destination telephone company, even if the toll charge is uncollectible.

This section of Phelps discloses the importance of telecommunications toll fraud prevention. Nowhere in this section, or elsewhere, does Phelps disclose or suggest generation of the predetermined pattern by a neural network, as required by claim 19. For at least these additional reasons, Applicants submit that claim 19 is not anticipated by Phelps.

Claim 20 recites that the at least one fraud detection test includes a comparison of at least a portion of the network event records to a predetermined pattern to identify a normal usage and/or a fraudulent usage, where the comparison is performed using tree-based algorithms that

[2] As Applicants' remarks with respect to the base independent claims are sufficient to overcome the Examiner's rejections of all claims dependent therefrom, Applicants' silence as to the Examiner's assertions with respect to dependent claims is not a concession by Applicants to the Examiner's assertions as to these claims, and Applicants reserve the right to analyze and dispute such assertions in the future.

generate discrete output values. Phelps does not disclose or suggest the combination of features recited in claim 20.

The Examiner alleged that Phelps discloses the features of claim 20, and cited col. 1, lines 15-20 of Phelps for support (Office Action, page 6). Col. 1, lines 15-22 of Phelps is reproduced above. This section of Phelps discloses the importance of telecommunications toll fraud prevention. Nowhere in this section, or elsewhere, does Phelps disclose or suggest performing a comparison using tree-based algorithms that generate discrete output values, as required by claim 20. For at least these additional reasons, Applicants submit that claim 20 is not anticipated by Phelps.

Claim 21 recites that the at least one fraud detection test includes a comparison of at least a portion of the network event records to a predetermined pattern to identify a normal usage and/or a fraudulent usage, where the comparison is performed using statistical based algorithms that that employ iterative numerical processing techniques. Phelps does not disclose or suggest the combination of features recited in claim 21.

The Examiner alleged that Phelps discloses the features of claim 21, and once again cited col. 1, lines 15-20 of Phelps for support (Office Action, page 6). Col. 1, lines 15-22 of Phelps is reproduced above. This section of Phelps discloses the importance of telecommunications toll fraud prevention. Nowhere in this section, or elsewhere, does Phelps disclose or suggest performing a comparison using statistical based algorithms that that employ iterative numerical processing techniques, as required by claim 21. For at least these additional reasons, Applicants submit that claim 21 is not anticipated by Phelps.

In light of the above, Applicants respectfully request the reconsideration and withdrawal of the Section 102(b) rejection of claims 1-5 and 7-27, as allegedly anticipated by Phelps.

REJECTION UNDER SECTION 103(a) BASED ON PHELPS

Claims 28-35 and 51-66 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Phelps. Applicants respectfully traverse this rejection.

Amended independent claim 28 is directed to a system for monitoring one or more of a plurality of credit card or debit card networks, each network being configured to generate network event records, each network event record being generated in response to an event occurring in the network. The system comprises a fraud detection system including a core computing infrastructure and a domain specific infrastructure. The domain specific infrastructure is dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored. The core computing infrastructure is non-domain specific. The fraud detection system is configured to analyze each network event record and perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on whether the network is a credit card system or a debit card system.

Phelps does not disclose or suggest the combination of features recited in claim 28. For example, Phelps does not disclose or suggest a system for monitoring one or more of a plurality of credit card or debit card networks, or a fraud detection system configured to analyze each network event record and perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on whether the network is a credit card network or a debit card network, as required by claim 28. Instead, Phelps discloses a fraud detection system for use in a telecommunications system to detect unauthorized use of billing numbers (col. 1, lines 6-10). Indeed, the words "debit card" do not appear in Phelps, and the words "credit card" only appear in Phelps in connection with a billing number of the

telecommunications system (col. 2, line 49). Nowhere does Phelps disclose or remotely suggest a system for monitoring one or more of a plurality of credit card or debit card networks, or a fraud detection system configured to analyze each network event record and perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on whether the network is a credit card network or a debit card network, as required by claim 28.

The Examiner alleged that Phelps teaches the fraud detection system recited in claim 28, and cited Fig. 2, col. 2, lines 40-62, and col. 1, lines 5-25 of Phelps for support (Office Action, page 8). Applicants respectfully disagree with the Examiner's interpretation of Phelps. Col. 2, lines 40-67 of Phelps is reproduced above and discusses Fig. 2. This section of Phelps discloses that the detection system detects fraudulent call activity (i.e., telecommunications) and generates alerts. Nowhere in this section, or elsewhere, does Phelps disclose or suggest a system for monitoring one or more of a plurality of credit card or debit card networks, or a fraud detection system configured to analyze each network event record and perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on whether the network is a credit card network or a debit card network, as required by claim 28.

Col. 1, lines 5-30 of Phelps discloses:

> 1. Field of the Invention
>
> The present invention relates to the field of telecommunications. More particularly, the invention is concerned with a detection system that analyzes call placement information concerning toll calls for detecting unauthorized use of billing numbers. In the preferred embodiment, a set of artificial intelligence rules operate on the call placement information to develop an indication that the use of a particular billing number is unauthorized.
>
> 2. Description of the Prior Art
>
> In the field of telecommunications toll fraud, it is important to have advanced toll fraud

> prevention techniques. Prevention is especially important when the unauthorized use is for international calls because the interexchange carrier handling the call may have to transfer payments to the destination telephone company, even if the toll charge is uncollectible.
>
> In response, interexchange carriers have instituted various toll fraud prevention schemes which are only partially successful, as illustrated by the fact that interexchange carriers will not place toll calls using a billing number to certain countries. Additionally, these schemes also prevent legitimate billing number calls and represent a loss of potential revenue to the carriers.

This section of Phelps discloses a detection system for a telecommunications system that analyzes calls and detects unauthorized use of billing numbers, and further discloses the importance of telecommunications toll fraud prevention. Nowhere in this section, or elsewhere, does Phelps disclose or suggest a system for monitoring one or more of a plurality of credit card or debit card networks, or a fraud detection system configured to analyze each network event record and perform a fraud prevention action in response to detecting an occurrence of fraud in the network event record and based on whether the network is a credit card network or a debit card network, as required by claim 28.

With regard to claim 28, the Examiner further alleged:

> Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Phelps and incorporate the method wherein a core computing infrastructure and a domain specific infrastructure, the domain specific infrastructure being dynamically reconfigurable in accordance with the domain specific implementation of the network being monitored in order to specify the type of computer being used.

(Office Action, page 9). With all due respect to the Examiner, Applicants find it difficult to follow the rationale of the preceding allegation. Furthermore, Applicants respectfully submit that this allegation represents nothing more than an impermissible generalization. In re Deuel, 51 F.3d 1552, 34 U.S.P.Q.2d 1210 (Fed. Cir. 1995) (holding that generalizations do not establish the realistic motivation to modify a specific reference in a specific manner to arrive at a specifically claimed invention).

For at least these reasons, Applicants submit that claim 28 is patentable over Phelps. Claims 29-35 and 51-66 depend from claim 28 and are, therefore, patentable over Phelps for at least the reasons given with regard to claim 28.[3] Claims 29-35 and 51-66 are also patentable over Phelps for reasons of their own.

For example, claim 56 recites that the fraud detection system includes a pattern recognition engine that includes a neural network configured to identify fraudulent patterns of usage. Phelps does not disclose or suggest the combination of features recited in claim 56.

The Examiner alleged that Phelps discloses the features of claim 56, and cited col. 1, lines 15-20 of Phelps for support (Office Action, page 12). Col. 1, lines 15-22 of Phelps is reproduced above and discloses the importance of telecommunications toll fraud prevention. Nowhere in this section, or elsewhere, does Phelps disclose or suggest that the fraud detection system includes a pattern recognition engine that includes a neural network configured to identify fraudulent patterns of usage, as required by claim 56. For at least these additional reasons, Applicants submit that claim 56 is patentable over Phelps.

Claim 57 recites that the fraud detection system includes a pattern recognition engine that includes tree-based algorithms. Phelps does not disclose or suggest the combination of features recited in claim 57.

The Examiner alleged that Phelps discloses the features of claim 57, and cited col. 1, lines 15-20 of Phelps for support (Office Action, page 12). Col. 1, lines 15-22 of Phelps is reproduced above and discloses the importance of telecommunications toll fraud prevention.

[3] As Applicants' remarks with respect to the base independent claims are sufficient to overcome the Examiner's rejections of all claims dependent therefrom, Applicants' silence as to the Examiner's assertions with respect to dependent claims is not a concession by Applicants to the Examiner's assertions as to these claims, and Applicants reserve the right to analyze and dispute such assertions in the future.

Nowhere in this section, or elsewhere, does Phelps disclose or suggest that the fraud detection system includes a pattern recognition engine that includes tree-based algorithms, as required by claim 57. For at least these additional reasons, Applicants submit that claim 57 is patentable over Phelps.

Claim 58 recites that the fraud detection system includes a pattern recognition engine that includes statistical based algorithms that employ iterative numerical processing techniques. Phelps does not disclose or suggest the combination of features recited in claim 58.

The Examiner alleged that Phelps discloses the features of claim 58, and once again cited col. 1, lines 15-20 of Phelps for support (Office Action, page 12). Col. 1, lines 15-22 of Phelps is reproduced above and discloses the importance of telecommunications toll fraud prevention. Nowhere in this section, or elsewhere, does Phelps disclose or suggest that the fraud detection system includes a pattern recognition engine that includes statistical based algorithms that employ iterative numerical processing techniques, as required by claim 58. For at least these additional reasons, Applicants submit that claim 58 is patentable over Phelps.

In light of the above, Applicants respectfully request the reconsideration and withdrawal of the Section 103(a) rejection of claims 28-35 and 51-66, as allegedly unpatentable over Phelps.

REJECTION UNDER SECTION 103(a) BASED ON PHELPS AND BOWMAN

Claims 6 and 36-50 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Phelps in view of Bowman. Applicants respectfully traverse this rejection.

Claim 6 depends from claim 1 and further recites that the at least one fraud detection test includes the step of normalizing the network event records such that the network event records conform to a predetermined format. Phelps and Bowman do not disclose or suggest the combination of features recited in claim 6. The Examiner admitted that "Phelps failed to

explicitly disclose the method, wherein the at least one fraud detection test includes the step of normalizing the network event record such that the network event record conforms to a predetermined format." (Office Action, page 15). However, the Examiner alleged that Bowman teaches such a normalizing step, and cited col. 7, lines 5-15 of Bowman for support (Office Action, page 15).

While not acquiescing in the Examiner's rejection, Applicants respectfully submit that the disclosure of Bowman does not cure the deficiencies in the disclosure of Phelps identified above with regard to claim 1. For example, Bowman does not disclose or suggest a method for detecting fraud in one of a credit card or debit card system, or performing at least one fraud detection test on the network event records based on whether the system is a credit card system or a debit card system, as required by claim 1 and claim 6 by virtue of its dependence on claim 1. Therefore, claim 6 is patentable over Phelps and Bowman, whether taken alone or in any reasonable combination, for at least the reasons given with regard to claim 1.

Claim 36 ultimately depends from claim 28 and further recites that a rules based thresholding engine further comprises: at least one rules database; a normalizer configured to configure the network event record into a standardized format; an enhancer component coupled to the normalizer, the enhancer component being configured to insert additional data in the network event record; and a threshold detector coupled to the enhancer component, the threshold detector being configured to compare a network event record to at least one threshold rule obtained from the at least one rules database, whereby the alarm is generated if the network event record violates the at least one threshold rule. Claims 37-50 depend, directly or indirectly, from claim 36.

Phelps and Bowman do not disclose or suggest the combination of features recited in

claims 36-50. The Examiner admitted that Phelps does not teach a normalizer configured to configure the network event record into a standardized format (Office Action, page 15). However, the Examiner alleged that Bowman teaches such a normalizer, and cited col. 7, lines 5-15 of Bowman for support (Office Action, page 16).

While not acquiescing in the Examiner's rejection, Applicants respectfully submit that the disclosure of Bowman does not cure the deficiencies in the disclosure of Phelps identified above with regard to claim 28. Therefore, claims 36-50 are patentable over Phelps and Bowman, whether taken alone or in any reasonable combination, for at least the reasons given with regard to claim 28.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants respectfully request the Examiner's reconsideration of the application and the timely allowance of pending claims 1-3, 5-33, and 35-66.

If the Examiner does not believe that all pending claims are now in condition for allowance, the Examiner is urged to contact the undersigned to expedite prosecution of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /James M. Olsen/
James M. Olsen
Reg. No. 40,408

Date: September 27, 2006
11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
Phone: (302) 478-4548
Fax: (571) 432-0808
CUSTOMER NUMBER: 25537